Przewodnik Rublon dotyczący gotowości do zapewnienia ciągłości biznesowej

Spis treści

1. Omówienie

Dlaczego potrzebujesz tego przewodnika:

Nawet najlepiej zaprojektowane usługi mogą czasem doświadczać zakłóceń w działaniu. Platforma Rublon MFA została zaprojektowana z myślą o wysokiej dostępności (posiada historię bezawaryjności przekraczającą 99,9%), jednak żadna usługa chmurowa nie jest całkowicie odporna na awarie.

Jakkolwiek rzadki, krótki okres niedostępności może mieć wpływ na dostęp użytkowników do krytycznych systemów. Takie przestoje mogą tymczasowo zakłócić produktywność pracowników, a nawet osłabić poziom bezpieczeństwa, jeśli nie zostaną odpowiednio opanowane.

Jako Twój zaufany dostawca uwierzytelniania wieloskładnikowego, Rublon chce przygotować Cię na każdą ewentualność. Ten poradnik pomoże Ci opracować plan utrzymania bezpiecznego dostępu podczas ewentualnych awarii lub degradacji usług Rublon. Zaplanuj działania z wyprzedzeniem, aby Twoja organizacja mogła sprawnie funkcjonować nawet wtedy, gdy platforma Rublon MFA napotka problem.

Zakres:

Poradnik koncentruje się na strategiach zapewnienia ciągłości działania usługi Rublon MFA. Wyjaśnimy:

- Różne rodzaje zakłóceń działania usług
- Jak zachowują się aplikacje zintegrowane z Rublon w każdym scenariuszu
- Jakie ustawienia konfiguracyjne i obejścia możesz zastosować

Przewodnik zawiera także przykładowe komunikaty, które pomogą Ci poinformować użytkowników końcowych podczas incydentu. Dzięki tej wiedzy możesz opracować dostosowany do potrzeb Twojej organizacji plan awaryjny.

2. Czy to Rublon MFA czy Twoja zapora sieciowa?

To, co wydaje się awarią usługi Rublon MFA, może w rzeczywistości być spowodowane czynnikami wewnętrznymi, takimi jak konfiguracja sieci.

Przeanalizuj, w jaki sposób chronione przez Rublon MFA aplikacje łączą się z interfejsem Rublon API i od jakich elementów infrastruktury zależą. Jeśli Twoja organizacja stosuje rygorystyczne reguły zapory sieciowej lub filtruje określony ruch, upewnij się, że usługa Rublon MFA jest przepuszczana. Rublon MFA działa w usłudze Amazon Web Services i korzysta ze statycznych adresów IP. Jeśli Twoja zapora nie została zaktualizowana o te adresy lub nie zezwala na komunikację z endpointem interfejsu Rublon API, może blokować żądania Rublon MFA, powodując błędy uwierzytelnienia, mimo że usługa Rublon MFA działa prawidłowo. (Innymi słowy, wewnętrzna błędna konfiguracja sieci może **sprawiać wrażenie** awarii Rublon MFA).

Aby zapobiec problemom w przyszłości, upewnij się, że Twoje środowisko jest odpowiednio przygotowane: skonfiguruj zaporę sieciową dla Rublon MFA. Upewnij się również, że spełnione są standardowe wymagania, takie jak poprawna konfiguracja DNS i obsługa protokołu TLS w wersji 1.2 lub wyższej, aby wszystkie systemy mogły połączyć się z serwerami Rublon MFA.

Wdrożenie powyższych kroków z wyprzedzeniem zapobiegnie wielu problemom z łącznością spowodowanymi przez czynniki środowiskowe i pomoże zapewnić nieprzerwaną komunikację usługi Rublon MFA z Twoimi aplikacjami.

3. Przygotowanie na awarie

Dobre przygotowanie jest kluczowe dla zminimalizowania skutków każdej awarii. Kiedy już zrozumiesz możliwe scenariusze przestojów i zachowanie każdej aplikacji (z Rublon lub bez), zdecydowanie zalecamy stworzenie **specyficznych planów odtworzeniowych dla każdej aplikacji** (Disaster Recovery, DR).

Każdy system chroniony przez Rublon może wymagać nieco innej procedury zapewnienia ciągłości działania. Zaplanowanie tych szczegółów zawczasu sprawi, że będzie można zareagować szybko i pewnie, jeśli dojdzie do awarii. Celem jest, by **nikt nie został zaskoczony** – administratorzy będą wiedzieli, co robić, a użytkownicy będą wiedzieli, czego się spodziewać.

Podczas opracowywania planów weź pod uwagę następujące kwestie:

- **Procedury przełączenia/pominięcia:** Opracuj i udokumentuj proces ręcznego pominięcia uwierzytelniania Rublon MFA lub „awaryjnego otwarcia" dostępu do aplikacji, jeśli usługa Rublon nie działa, a automatyczne przełączenie nie zadziałało. Może to obejmować zmianę ustawień, modyfikację klucza rejestru lub zmianę ścieżki uwierzytelniania, tak aby tymczasowo pominąć uwierzytelnianie Rublon MFA. Dowiedz się zawczasu, jak szybko aktywować te opcje pominięcia oraz jak ustawić tryb Fail Mode w konektorach Rublon.

- **Zachęcanie do wielu metod MFA:** W ramach standardowego procesu wdrażania nowych użytkowników poproś każdego użytkownika o zarejestrowanie co najmniej dwóch metod MFA (np. powiadomienie push na telefon, kod jednorazowy TOTP, SMS, e-mail, klucz bezpieczeństwa FIDO). Dzięki temu, jeśli jedna metoda ulegnie awarii, użytkownicy będą mogli przełączyć się na inną bez konieczności tworzenia zgłoszeń do helpdesku.

- **Kroki wyłączenia/usunięcia:** Opisz, jak usunąć usługę Rublon z procesu uwierzytelnienia dla każdej chronionej aplikacji, jeśli będzie to absolutnie konieczne. Może to oznaczać odinstalowanie lub wyłączenie konektora Rublon, dezaktywację ustawienia wymuszania uwierzytelniania MFA w konsoli Rublon Admin Console albo powrót do lokalnej metody logowania. Zidentyfikuj te kroki oraz wymagane uprawnienia z wyprzedzeniem, aby administrator mógł je wykonać pod presją czasu.

- **Odpowiedzialny personel:** Ustal, kto w Twojej organizacji odpowiada za zapewnienie ciągłości działania. Upewnij się, że osoby te mają dostępy i poświadczenia potrzebne by wprowadzać zmiany w konfiguracji (np. dostęp do serwerów, na których zainstalowane

są konektory Rublon, konto administratora w konsoli Rublon itp.). Warto, by więcej niż jedna osoba znała plan na wypadek, gdyby główny wykonawca nie był dostępny.

- **Testy i ćwiczenia:** Nie czekaj na prawdziwy incydent, aby przekonać się, czy Twój plan działa. Jeśli to możliwe, przetestuj procedury przełączenia na tryb awaryjny w kontrolowanych warunkach (np. symulując awarię usługi Rublon w środowisku testowym). Regularne ćwiczenia pozwolą upewnić się, że udokumentowane kroki faktycznie umożliwiają logowanie, gdy usługa Rublon jest nieosiągalna, a personel nabierze wprawy w ich wykonywaniu. Jeżeli podczas testu okaże się, że coś w planie nie działa, zaktualizuj odpowiednio dokumentację.

- **Plan komunikacji:** Ustal, jak będziesz komunikować się z zespołami IT oraz użytkownikami końcowymi podczas awarii. (W dalszej części poradnika podajemy przykładowe komunikaty dla użytkowników.) Posiadanie gotowych wzorów wiadomości oraz wewnętrznego procesu powiadamiania pozwoli zaoszczędzić cenny czas, gdy liczy się każda minuta. Przygotuj również podstawowe i zapasowe kanały komunikacji, takie jak powiadomienia e-mail czy dedykowane kanały czatu, tak aby w razie awarii głównego kanału istniała niezawodna alternatywa. Ustal solidny proces przekazywania komunikatów, wraz z procedurami awaryjnymi, by jeszcze bardziej zwiększyć gotowość na wypadek awarii.

4. Decyzje konfiguracyjne: tryb Fail Safe vs. Fail Secure

Kluczowym elementem planowania ciągłości działania jest decyzja, jak każda aplikacja powinna zachować się w sytuacji, gdy usługa Rublon stanie się niedostępna. Większość konektorów Rublon umożliwia skonfigurowanie trybu **Fail Mode**, pozwalając zasadniczo na wybór między podejściem „**awaryjnie otwartym**” (pozwól na dostęp) a „**awaryjnie zamkniętym**” (odmów dostępu) w sytuacji, gdy nie można dokończyć procesu MFA. Te tryby nazywamy odpowiednio **Fail Safe** (obejście, pominięcie) i **Fail Secure** (odmowa dostępu, odrzucenie). Wybór trybu dla danej aplikacji polega na wyważeniu bezpieczeństwa oraz dostępności i powinien być zgodny z polityką Twojej organizacji. (Szczegółowe omówienie zachowania trybów awaryjnych znajdziesz w sekcji 7.)

Większość konektorów Rublon pozwala na konfigurację zachowania w trybie Fail Mode. W kolejnych rozdziałach omówimy, co dzieje się przy każdym typie awarii i jak działa wówczas tryb Fail Mode. Miej na uwadze, który tryb jest ustawiony (lub będzie ustawiony) dla każdej aplikacji i udokumentuj te decyzje, ponieważ bezpośrednio wpływają one na Twój plan działania w razie awarii.

Wybierając tryb Fail Mode dla aplikacji, należy wziąć pod uwagę następujące czynniki:

- **Wymagania polityk i zgodności:** Czy obowiązujące przepisy lub wewnętrzne polityki bezpieczeństwa **wymagają** zablokowania dostępu, jeśli nie można wywołać uwierzytelniania MFA? Na przykład niektóre standardy nakazują stosowanie uwierzytelniania MFA w określonych systemach przez cały czas. W takim przypadku tryb Fail Secure (odmowa dostępu bez MFA) jest koniecznością dla tych systemów. Z drugiej strony, w środowiskach mniej regulowanych można dopuścić użycie trybu Fail Safe (pominięcie MFA), aby utrzymać ciągłość pracy. Decyzję tę należy udokumentować i okresowo rewidować w miarę zmian przepisów i priorytetów organizacji.
- **Wrażliwość danych i systemów:** Oceń, jakiego typu dane i zasoby chroni dana aplikacja. Dla systemów zawierających bardzo wrażliwe informacje (np. dane finansowe, dane medyczne czy kontrola infrastruktury krytycznej) należy przedkładać bezpieczeństwo nad dostępność, skłaniając się ku trybowi Fail Secure, aby zminimalizować ryzyko nieautoryzowanego dostępu. W przypadku aplikacji zawierających bardziej ogólne dane

o niskim ryzyku, można priorytetyzować dostępność poprzez Fail Safe, tak by użytkownicy mogli kontynuować pracę podczas awarii.

- **Grupy użytkowników i poziomy dostępu:** Jedno uniwersalne ustawienie może nie pasować do wszystkich przypadków. Możesz mieć różne grupy użytkowników o odmiennych profilach ryzyka. Przykładowo, od użytkowników uprzywilejowanych możesz wymagać trybu Fail Secure (bez pomijania MFA), podczas gdy ogół personelu uzyskujący dostęp do mniej krytycznych systemów mógłby mieć ustawiony tryb Fail Safe.

- **Równowaga między bezpieczeństwem a użytecznością:** Przeanalizuj jaki wpływ na użytkowników ma odmówienie im dostępu oraz jak to się ma do wpływu na bezpieczeństwo, jeśli uwierzytelnianie MFA zostanie pominięte. Tryb Fail Safe (pominięcie) zapewnia, że użytkownicy nigdy nie utracą dostępu do swoich systemów z powodu awarii usługi MFA. Poprawia to ciągłość pracy i produktywność, ale kosztem tymczasowego braku drugiego czynnika uwierzytelnienia. Z kolei tryb Fail Secure utrzymuje wymóg MFA przez cały czas, zachowując wysoki poziom bezpieczeństwa, lecz potencjalnie kosztem tego, że użytkownicy nie będą mogli się zalogować, dopóki usługa MFA nie zostanie przywrócona. Możesz wybrać tryb Fail Safe dla systemów, gdzie nieprzerwany dostęp jest absolutnym priorytetem (np. stacje robocze z systemem Windows), a tryb Fail Secure dla systemów, w których obejście MFA stanowiłoby niedopuszczalne ryzyko (np. dostęp VPN do sieci produkcyjnej).

5. Rodzaje awarii

Nie wszystkie przerwy w działaniu usługi wyglądają tak samo. Zakłócenia działania usługi Rublon MFA można podzielić na dwie ogólne kategorie:

- **Interfejs Rublon API jest nieosiągalny** – całkowita awaria, w której konektory Rublon nie mogą skontaktować się z interfejsem Rublon API. Zazwyczaj uruchamia to skonfigurowany w konektorze tryb Fail Mode (Fail Safe lub Fail Secure), automatycznie przepuszczając użytkowników lub odmawiając im dostępu.
- **Degradacja usługi Rublon** - częściowe zakłócenie działania, w którym interfejs Rublon API jest co prawda osiągalne, ale niektóre usługi Rublon działają wolno, zawodnie albo są niedostępne. Tryb Fail Mode nie uruchamia się automatycznie, więc administratorzy mogą być zmuszeni do manualnej interwencji.

Dlaczego rozróżniamy nieosiągalność i degradację?

Przede wszystkim dlatego, że Twoja odpowiedź będzie się różnić. Jeśli Rublon jest całkowicie nieosiągalny, znaczna część planu ciągłości działania oprze się na **ustawieniach Fail Safe lub Fail Secure**, które skonfigurowano zawczasu. Natomiast w przypadku degradacji usługi może być potrzebna aktywna interwencja (np. zakomunikowanie użytkownikom sposobu na obejście problemu lub tymczasowa zmiana ustawień), ponieważ system nie przełączy się automatycznie na tryb awaryjny. Pamiętaj o tych kategoriach i zastanów się, jak każda z Twoich aplikacji powinna zachowywać się w każdym scenariuszu.

Interfejs Rublon API jest nieosiągalny

Ten scenariusz zakłada całkowite przerwanie łączności z interfejsem Rublon API. Oznacza to, że Twoje konektory Rublon **w ogóle nie mogą nawiązać połączenia z interfejsem Rublon API (np. otrzymują kod HTTP 404), albo co prawda nawiązały połączenie, ale otrzymują odpowiedzi z kodem błędu HTTP 5xx (500–599)**. W takiej sytuacji uruchamia się tryb Fail Mode.

Gdy interfejs Rublon API jest nieosiągalny, widok Rublon Prompt (ekran monitujący o uwierzytelnienie drugim czynnikiem) nie załaduje się podczas logowania albo – w integracjach niewspierających tego widoku – żądanie do interfejsu Rublon API przekroczy limit czasu. Konektory Rublon zwykle czekają określony czas na odpowiedź, po czym uznają

interfejs Rublon API za nieosiągalny. W tym momencie włącza się skonfigurowany tryb **Fail Mode** konektora, automatycznie umożliwiając lub odmawiając dostępu użytkownikom, zgodnie z wybranym ustawieniem. Często nazywamy ten scenariusz „przełączeniem awaryjnym", ponieważ konektor przełącza się na swój zdefiniowany tryb (otwarty/pominięcie lub zamknięty/odmowa).

Przyczyny zdarzenia „interfejs Rublon API jest nieosiągalny" mogą obejmować:

- **Przestój usługi Rublon:** Interfejs Rublon API jest chwilowo wyłączony lub nie odpowiada. Jest to rzadkie, ale może się zdarzyć (np. z powodu zaplanowanej konserwacji).
- **Problemy z połączeniem sieciowym:** Problemy na ścieżce sieciowej między Twoim środowiskiem a interfejsem Rublon API mogą spowodować brak dostępu do usługi. Często źródło problemów leży po stronie klienta lub w infrastrukturze internetowej. Przykłady to awaria dostawcy internetu lub problem z routingiem, awaria DNS przy rozwiązywaniu domen Rublon, czy zdarzenie losowe (np. przerwanie światłowodu) powodujące zerwanie łączności. Często zdarzają się również błędy w lokalnej konfiguracji, np. zmiana reguły zapory sieciowej lub problem z serwerem proxy może nagle zacząć blokować ruch do Rublon, sprawiając, że usługa wydaje się nieosiągalna.
- **Błędna konfiguracja integracji:** Jeśli konektor Rublon jest niepoprawnie skonfigurowany, może nie być w stanie połączyć się z interfejsem Rublon API. Przykładowo, nieprawidłowa wartość Rublon System Token lub Secret Key w konfiguracji może spowodować niepowodzenie zapytań uwierzytelnienia. W takiej sytuacji konektor potraktuje brak odpowiedzi podobnie jak sytuacje, w której usługa jest nieosiągalna, ponieważ nigdy nie otrzyma prawidłowej odpowiedzi. Podobnie, użycie przestarzałej, niekompatybilnej wersji konektora Rublon może skutkować błędami w komunikacji z usługą.

Degradacja usługi Rublon

Ten termin oznacza częściowe problemy z usługą, gdzie interfejs Rublon API jest **wciąż osiągalny**, ale pewne elementy usługi MFA nie funkcjonują poprawnie. Podczas degradacji aplikacje nadal mogą kontaktować się z Rublon (więc konektory nie uruchamiają trybu Fail Mode), ale użytkownicy mogą doświadczać błędów lub opóźnień przy próbie uwierzytelnienia za pomocą uwierzytelniania MFA.

W scenariuszu degradacji **konektory nie uruchamiają automatycznie trybu Fail Mode**, ponieważ interfejs Rublon API wciąż odpowiada (nawet jeśli z opóźnieniem). Osoby odpowiedzialne za ciągłość działania muszą rozpoznać oznaki degradacji usługi (np. liczne zgłoszenia użytkowników, że ich kody SMS czy e-maile z linkami nie dochodzą) i zdecydować, czy potrzebne jest podjęcie działań, takich jak ręczne czasowe pominięcie wymogu MFA na czas trwania problemu.

Przykłady degradacji obejmują:

- **Awaria konkretnej metody:** Jedna lub więcej metod drugiego czynnika nie działa, podczas gdy pozostałe działają poprawnie. Na przykład, być może dostawca usług telefonicznych Rublon do obsługi wiadomości SMS lub połączeń telefonicznych ma awarię, więc kody SMS nie są dostarczane użytkownikom. Tymczasem inne metody, takie jak Powiadomienie mobilne czy klucze bezpieczeństwa FIDO, nadal działają.
- **Częściowa awaria lub spowolnienie:** Infrastruktura Rublon może być pod dużym obciążeniem lub doświadczać lokalnego problemu, który zwiększa opóźnienie podczas uwierzytelniania. Użytkownicy mogą zauważyć, że monity drugiego czynnika pojawiają się wolniej niż zwykle albo czasami zawodzą, ale ostatecznie żądania przechodzą. Może się tak zdarzyć, jeśli jeden komponent infrastruktury chmury Rublon (np. konkretny klaster serwerów) boryka się z problemami, podczas gdy pozostałe nadal działają. Użytkownicy mogą zgłaszać, że „MFA się zawiesza” lub że muszą próbować logowania wielokrotnie, aby się w końcu udało.
- **Problemy programowe:** W niezwykle rzadkich przypadkach błąd oprogramowania może spowodować degradację usługi. Na przykład jeśli nowa wersja wprowadziła błąd, część prób uwierzytelnienia może kończyć się niepowodzeniem (mimo że usługa technicznie „działa”). Mamy nadzieję, że takie zdarzenia nigdy nie wystąpią, ale warto mieć świadomość, że są możliwe – usługa technicznie działa, lecz nie w pełni poprawnie.

6. Wykrywanie awarii

Skąd masz wiedzieć, że występuje awaria? Wczesne wykrycie ma kluczowe znaczenie. Dzięki czujnemu monitorowaniu z wykorzystaniem poniższych kroków szybko zauważysz awarię i określisz jej charakter (czy to nieosiągalność czy degradacja). Szybkie wykrycie pozwoli Ci szybciej uruchomić plan awaryjny.

Oto kroki i narzędzia, które pomogą Ci szybko rozpoznać problem z usługą Rublon:

- **Monitoruj stronę statusu Rublon:** Pod adresem status.rublon.com, Rublon udostępnia stronę monitorującą infrastrukturę w czasie rzeczywistym. Ta strona powinna być Twoim pierwszym przystankiem, gdy podejrzewasz, że wystąpił powszechny problem. Strona statusu raportuje kondycję kluczowych komponentów, takich jak interfejs Rublon API, konsola administracyjna, portal wsparcia, witryna internetowa, a nawet poszczególne funkcje, takie jak wysyłanie SMS/połączeń telefonicznych/e-mail. Jeśli dowiemy się o zakłóceniu w działaniu usługi lub planowanej konserwacji, zamieścimy informacje na naszej stronie statusu. Z tego powodu zalecamy subskrypcję aktualizacji. Dzięki temu otrzymasz powiadomienie, gdy tylko wystąpi incydent. Subskrybowanie gwarantuje, że nie przegapisz krytycznych ogłoszeń o awariach czy pracach serwisowych.
- **Diagnostyka lokalna:** Jeśli doświadczasz problemów, ale strona statusu wskazuje, że wszystkie usługi Rublon działają, problem może leżeć po Twojej stronie lub po stronie sieci pośredniczącej. Oto kilka kroków diagnostycznych:
    - **Sprawdź łączność z interfejsem Rublon API:** Spróbuj połączyć się z punktem końcowym interfejsu Rublon API ze swojego środowiska. Na przykład otwórz przeglądarkę na maszynie, na której występują problemy i przejdź do strony **https://core.rublon.net**. Ten adres URL to główny serwer uwierzytelniania Rublon. Jeśli jest osiągalny, w przeglądarce zobaczysz prosty komunikat, np. *„Rublon Authentication Server works!” („Serwer uwierzytelniający Rublon działa!”)*. Wykonaj ten test z kilku różnych sieci i urządzeń. Jeżeli w jednej sieci pojawia się komunikat „działa”, a w innej nie, sugeruje to problem sieciowy (np. zapora lub routing) w sieci, w której test się nie powiódł. Ten test pomoże ustalić, czy Rublon rzeczywiście nie działa, czy też coś w Twoim środowisku blokuje dostęp.
    - **Traceroute/DNS:** Standardowe narzędzia sieciowe mogą pomóc zidentyfikować problem. Użyj polecenia **tracert/traceroute** dla adresu **core.rublon.net,** aby sprawdzić, czy ruch dociera do internetu. Sprawdź również poleceniem **nslookup**

core.rublon.net czy rozwiązywanie nazw DNS zwraca adres IP. Jeżeli zapytanie DNS nie daje wyniku albo trasa pakietów zatrzymuje się wewnątrz Twojej sieci, najprawdopodobniej występuje u Ciebie problem lokalny.

- **Logi zapory/proxy:** Jeśli korzystasz z serwera proxy lub zapory sieciowej, sprawdź logi tych urządzeń z czasu występowania problemów. Możesz odkryć, że połączenia do domen/adresów IP usługi Rublon są odrzucane lub blokowane. Upewnij się, że komunikacja wychodząca do **core.rublon.net** przez port TCP 443 jest dozwolona. Jeśli Twoja zapora korzysta z listy dozwolonych adresów, upewnij się, że adresy IP usługi Rublon MFA są dozwolone. Jeśli Twoja polityka sieciowa umożliwia filtrowanie po FQDN, zezwól na **core.rublon.net**. Zwróć szczególną uwagę na wszelkie niedawne zmiany w konfiguracji zapory oraz na alerty systemów IDS/IPS, które zbiegły się w czasie z awarią.

- **Rozróżnienie pomiędzy problemem powszechnym a izolowanym**: Ustal, czy problem dotyczy wszystkich użytkowników i aplikacji, czy tylko niektórych. Jeśli **wszystkie próby uwierzytelnienia kończą się niepowodzeniem**, wskazuje to na szerszą awarię (całkowity brak dostępu do interfejsu Rublon API lub poważna awaria sieci). Jeżeli zawodzi tylko określona metoda lub aplikacja, może to być degradacja usługi lub problem specyficzny dla tej aplikacji. Przykładowo, jeśli nie docierają jedynie kody SMS, ale powiadomienia push i e-maile działają poprawnie, najprawdopodobniej mamy do czynienia z degradacją usługi Rublon w kanale SMS (lub awarią u dostawcy SMS). Jeśli problemy występują tylko z Twoją usługą VPN (korzystającą z usługi Rublon Authentication Proxy), a logowanie do systemu Windows chronione przez Rublon przebiega normalnie, problem może być ograniczony do samego proxy lub jego konfiguracji.

- **Skontaktuj się ze wsparciem technicznym Rublon Support:** Jeżeli po wykonaniu powyższych kroków nadal nie masz pewności lub potrzebujesz pomocy, nie wahaj się skontaktować ze wsparciem technicznym Rublon Support. W zgłoszeniu podaj jak najwięcej szczegółów (co zawodzi, komunikaty błędów, zrzuty ekranu oraz istotne fragmenty logów).

7. Tryb Rublon Fail Mode

Konektory Rublon zawierają mechanizm zwany trybem Fail Mode, który kontroluje, co konektor powinien zrobić, jeśli nie uda mu się dokończyć procesu uwierzytelniania MFA.

Tryb Fail Mode może przyjąć następujące wartości:

- **Fail Safe (pominięcie)** – jeśli interfejs Rublon API stanie się nieosiągalny, użytkownicy **zostaną dopuszczeni** do aplikacji zintegrowanych z usługą Rublon, o ile przejdą uwierzytelnienie podstawowe.
- **Fail Secure (odrzucenie)** - jeśli interfejs Rublon API stanie się nieosiągalny, użytkownikom **odmówi się dostępu** do aplikacji zintegrowanych z usługą Rublon, nawet jeśli ukończą uwierzytelnienie podstawowe.

Oba tryby – Fail Safe i Fail Secure – mają swoje zastosowania. Rublon zapewnia Ci elastyczność decydowania o tym, którego trybu użyć dla każdego konektora. Możliwe jest nawet mieszanie trybów: np. możesz ustawić większość konektorów na Fail Safe, a kilka najbardziej wrażliwych na Fail Secure. Kluczem jest skonfigurowanie tych ustawień z wyprzedzeniem i udokumentowanie swoich wyborów, aby zawsze być gotowym zarówno na planowane prace serwisowe, jak i nieplanowaną awarię.

Tryb Fail Safe („przepuść przy braku połączenia”)

Tryb **Fail Safe** oznacza, że jeśli interfejs Rublon API jest nieosiągalny, **użytkownik może się zalogować bez dokańczania procesu MFA**. Innymi słowy, pomijany jest krok drugiego czynnika i żeby przyznać dostęp wystarczą same podstawowe dane uwierzytelniające (zwykle nazwa użytkownika i hasło).

- **Priorytet:** Tryb Fail Safe kładzie nacisk na dostępność. Użytkownicy mogą kontynuować pracę nawet w sytuacji awarii usługi MFA. Warto jednak pamiętać, że tryb Fail Safe okupiony jest obniżeniem poziomu bezpieczeństwa na czas awarii (ponieważ użytkownicy nie są wtedy weryfikowani drugim czynnikiem).
- **Zachowanie:** Z perspektywy użytkownika końcowego zdarzenie Fail Safe wygląda jak zwykłe logowanie, z tą różnicą, że nie pojawia się w nim żaden monit o podanie drugiego czynnika. Na przykład pracownik loguje się do swojego laptopa z systemem Windows jak

zwykle, wpisując nazwę użytkownika i hasło, po czym – zamiast zobaczyć widok Rublon Prompt – logowanie od razu kończy się sukcesem. Oznacza to, że system go przepuścił (pominął wymóg MFA).

- **Kiedy stosować:** Tryb Fail Safe jest generalnie zalecany dla systemów, w których utrzymanie dostępu jest ważniejsze niż egzekwowanie uwierzytelniania MFA w danym momencie. Wiele organizacji wybiera tryb Fail Safe dla systemów używanych bezpośrednio przez pracowników, np. stacji roboczych czy wewnętrznych aplikacji, aby uniknąć odcięcia pracowników. Jeśli wdrażasz tryb Fail Safe, upewnij się, że masz wdrożone inne zabezpieczenia (np. silne uwierzytelnianie podstawowe, monitoring sieci, solidne mechanizmy kontroli dostępu itp.), aby zrekompensować tymczasowy brak uwierzytelniania MFA podczas przestoju.
- **Konfiguracja:** Każdy konektor Rublon ma własny sposób ustawienia trybu Fail Safe (zwykle parametr konfiguracyjny **FailMode** ustawiony na **„bypass”**). Domyślnie konektory Rublon działają w trybie Fail Safe, aby uniknąć zablokowania administratorów podczas początkowej konfiguracji. Aby zmienić to ustawienie w poszczególnych konektorach, zobacz Jak ustawić tryb Fail Mode w konektorach Rublon?. Jeżeli zdecydujesz się pozostać przy trybie Fail Safe, warto przetestować jego działanie (np. tymczasowo blokując dostęp konektora do internetu w środowisku testowym), aby potwierdzić, że rzeczywiście pomija on uwierzytelnianie MFA zgodnie z oczekiwaniami.

Tryb Fail Secure („odrzuć przy braku połączenia”)

Tryb **Fail Secure** oznacza, że jeśli interfejs Rublon API jest nieosiągalny, **użytkownik nie zostanie wpuszczony**. W tym trybie użytkownik, który poprawnie wpisał swoje podstawowe dane logowania i tak **zostanie zablokowany, jeśli nie można zweryfikować drugiego czynnika**.

Wpływ zastosowania trybu Fail Secure jest prosty: brak dostępu do interfejsu Rublon API = brak możliwości logowania. Maksymalizuje to bezpieczeństwo kosztem ciągłego dostępu. Jeśli wybierzesz ten tryb dla jakiejś aplikacji, upewnij się, że **Twój plan ciągłości działania przewiduje, jak poradzić sobie z potencjalnym przestojem**. Może to oznaczać przekazanie użytkownikom informacji, by zaczekali, lub zastosowanie obejścia w postaci alternatywnej metody logowania (np. awaryjne lokalne konto, które nie korzysta z Rublon, choć to z kolei przychodzi ze swoim własnym ryzykiem). W wielu przypadkach organizacje stosują tryb Fail Secure w systemach z ograniczoną bazą użytkowników lub tam, gdzie przestój, choć uciążliwy, jest akceptowalny w porównaniu z ryzykiem nieautoryzowanego dostępu.

- **Priorytet:** Ten tryb stawia na bezpieczeństwo – nigdy nie pozwoli nikomu zalogować się bez usługi MFA. Odbywa się to jednak kosztem dostępności aplikacji podczas awarii (ponieważ nawet uprawnieni użytkownicy będą zablokowani, dopóki uwierzytelnianie MFA znów nie zacznie działać).

- **Zachowanie:** W scenariuszu Fail Secure użytkownicy zostaną pozbawieni dostępu, jeśli nie będzie można nawiązać połączenia z interfejsem Rublon API. Po wpisaniu nazwy użytkownika i hasła usługa Rublon, natychmiast wyświetli komunikat w rodzaju *„Access Denied!" („Dostęp zabroniony!")*. Może to być frustrujące, jeśli użytkownik się tego nie spodziewa. Nie zrobił nic złego, a mimo to nie ma dostępu z powodu ustawienia dotyczącego uwierzytelniania MFA. Dlatego kluczowe jest poinformowanie użytkowników o konsekwencjach trybu Fail Secure podczas awarii.

- **Kiedy stosować:** Tryb Fail Secure jest odpowiedni dla systemów o wysokim poziomie bezpieczeństwa, gdzie zablokowanie dostępu jest preferowane do wpuszczenia użytkownika zweryfikowanego tylko uwierzytelnianiem podstawowym. Jeżeli aplikacja chroni wrażliwe dane lub stanowi bramę do rozległej sieci, możesz zdecydować, żeby zawsze wymagała uwierzytelniania MFA, nawet jeśli oznacza to akceptację przestoju podczas planowych prac serwisowych Rublon. Niektóre organizacje ustawiają tryb Fail Secure na zewnętrznych punktach dostępowych, takich jak sieci VPN czy uprzywilejowane portale administracyjne IT. Zanim wybierzesz tryb Fail Secure, rozważ:

    - Jak ważne jest, aby ten system pozostał dostępny?
    - Czy istnieją alternatywne sposoby dostania się do systemu, jeśli uwierzytelnianie MFA nie działa (np. awaryjne lokalne konto administratora lub dostęp przez konsolę)?
    - Czy użytkownicy będą wiedzieć, że awaria usługi MFA oznacza „proszę czekać, w tej chwili nie można się zalogować"?

- **Konfiguracja:** Włączenie trybu Fail Secure polega na ustawieniu trybu Fail Mode na „deny" (odmowa). Szczegółowe instrukcje dla poszczególnych konektorów znajdziesz w Jak ustawić tryb Fail Mode w konektorach Rublon?. Warto przetestować zachowanie trybu Fail Secure (np. tymczasowo blokując konektorowi dostęp do internetu w środowisku testowym), aby potwierdzić, że rzeczywiście odmawia dostępu zgodnie z oczekiwaniami.

8. Obsługa trybu Fail Mode w integracjach Rublon

Integracje Rublon (aplikacje, wtyczki i konektory), które umożliwiają konfigurację trybu Fail Mode:

- Rublon Authentication Proxy
- Rublon Access Gateway
- Rublon MFA dla Windows Logon & RDP
- Rublon MFA dla Remote Desktop Gateway
- Rublon MFA dla RD Web Access
- Rublon MFA dla RD Web Client
- Rublon MFA dla Outlook Web App (OWA)
- Rublon MFA dla Active Directory Federation Services (AD FS)
- Rublon MFA dla Linux SSH
- Rublon MFA dla Veritas NetBackup
- Rublon MFA dla Jira
- Rublon MFA dla Confluence

Integracje Rublon, które **nie umożliwiają** konfiguracji trybu Fail Mode:

- Rublon MFA dla Roundcube
- Rublon MFA dla WordPress

Szczegółowe instrukcje dotyczące ustawiania trybu Fail Mode w każdym konektorze można znaleźć w:

Jak ustawić tryb Fail Mode w konektorach Rublon?

9. Scenariusze i opcje reakcji na niedostępność interfejsu Rublon API

Interfejs Rublon API może być nieosiągalny na różne sposoby: może być niedostępny dla wszystkich (interfejs nie jest osiągalny z żadnej sieci ani lokalizacji) lub być niedostępny tylko dla niektórych konektorów lub lokalizacji (często z powodu błędnej konfiguracji zapory lub sieci). W obu przypadkach konektor nie otrzymuje prawidłowej odpowiedzi i zastosowuje ustawiony tryb Fail Mode.

Komunikacja i monitoring mają kluczowe znaczenie:

Informuj na bieżąco swój zespół bezpieczeństwa IT oraz kierownictwo o tymczasowych rozwiązaniach, które stosujesz. Na przykład, jeśli ustawiono wszystkim użytkownikom z działu finansów pominięcie uwierzytelniania MFA, poinformuj o tym oficera bezpieczeństwa. Może to oznaczać zwiększone ryzyko, na które powinni wyrazić zgodę. Po fakcie zanotuj lub zgłoś, co zostało zrobione (np. „O 10:00 z powodu awarii usługi Rublon ustawiono VPN na tryb bypass”). Pomoże to w późniejszych analizach incydentu
i audytach.

Poinformuj także zespół helpdesku i użytkowników, że jesteś świadomy problemu oraz jaki tryb awaryjny jest w użyciu:

- Jeśli korzystasz z trybu **Fail Safe** (pominięcie), użytkownicy mogą być zaskoczeni lub zaniepokojeni, że nie są proszeni o uwierzytelnienie MFA.
- Jeśli korzystasz z trybu **Fail Secure** (odrzucenie), użytkownicy mogą być zaskoczeni, że nie mają dostępu do swoich aplikacji.
- Szybka wiadomość może zaoszczędzić wielu nieporozumień. W dalszej części tego przewodnika podajemy przykładowe komunikaty dla użytkowników.

Przykład: Interfejs Rublon API jest nieosiągalny. Nie można się z nim połączyć z żadnej sieci ani punktu końcowego. Interfejs Rublon API jest nieosiągalny dla wszystkich konektorów Rublon.

Skutek:

- Jeśli ustawiono tryb Fail Secure, użytkownicy nie mogą dokończyć uwierzytelnienia MFA.
- Jeśli ustawiono tryb Fail Safe, użytkownicy są wpuszczani (bez MFA).

Wykrycie: Strona statusu Rublon będzie wskazywać na problemy z interfejsem Rublon API. Jeżeli strona statusu nie pokazuje żadnych problemów z interfejsem Rublon API, bardzo mocno sugeruje to problem z konfiguracją konektora lub nieprawidłowo skonfigurowaną zaporę sieciową.

Opcje reakcji:

- **Przełącz na tryb pominięcia (Fail Safe):** Jeśli normalnie dana aplikacja działa w trybie Fail Secure, jednym z szybkich obejść podczas awarii jest zmiana trybu na Fail Safe. Można to zrobić, zmieniając ustawienie trybu Fail Mode na „bypass" (pominięcie). Przykładowo, jeśli usługa Rublon Authentication Proxy pracuje w trybie **„deny"**, edytuj plik konfiguracyjny, ustaw **fail_mode: "bypass"** i zrestartuj usługę proxy. W efekcie do czasu powrotu do normy użytkownicy będą wpuszczani bez MFA. Wielu administratorów robi to proaktywnie, gdy widzi nadchodzący przestój (na przykład gdy ogłaszamy przerwę serwisową). **Zanotuj jednak dokładnie, gdzie wprowadzono takie zmiany, aby można było je cofnąć po zakończeniu incydentu. Nie chcesz przypadkowo pozostawić aplikacji w trybie stałego pominięcia, co stanie się luką w zabezpieczeniach.**
- **Dostosuj zaporę sieciową/sieć:** Jeśli odkryjesz, że problem wynika z tego, iż Twoja zapora lub sieć blokuje ruch do interfejsu Rublon API (na przykład nowa reguła zapory uniemożliwiła dostęp do **core.rublon.net)**, obejściem będzie jak najszybsze usunięcie tej przeszkody. Może to obejmować:
  - Otwarcie portu wychodzącego 443 i dodanie adresu **https://core.rublon.net** do listy dozwolonych.
  - Dodanie najnowszych zakresów adresów IP usługi Rublon do zapory.
  - Tymczasowe wyłączenie restrykcyjnej reguły (za odpowiednimi zgodami) do czasu, aż będzie można ją udoskonalić, aby zezwolić na ruch Rublon.
  - Dowiedz się więcej: Jak skonfigurować zaporę sieciową dla usługi Rublon?

10. Scenariusze i opcje reakcji na degradację usługi

Gdy infrastruktura Rublon działa w stanie częściowej degradacji, może być konieczne podjęcie dodatkowych kroków, by zminimalizować zakłócenia. W przeciwieństwie do pełnej awarii, degradacja oznacza, że uwierzytelnianie MFA nadal w pewnym stopniu działa, więc automatyczne przełączenie na tryb Fail Mode **nie zadziała**.

Komunikacja i monitoring mają kluczowe znaczenie:

Poinformuj dział pomocy technicznej i użytkowników, że wiesz o problemie i jakie rozwiązania należy zastosować. Użytkownicy napotykający trudności z uwierzytelnianiem MFA mogą bez końca ponawiać próby lub założyć, że to wina ich urządzenia. Krótki komunikat może oszczędzić wiele zamieszania. W dalszej części tego przewodnika podajemy kilka przykładowych komunikatów dla użytkowników.

Jeżeli degradacja dotyczy tylko jednego specyficznego konektora lub integracji:

Na przykład tylko logowanie MFA w Twojej sieci VPN zawodzi, podczas gdy inne aplikacje korzystające z platformy Rublon działają normalnie. W takim przypadku Twój plan awaryjny może polegać na przełączeniu tylko tej jednej aplikacji w tryb awaryjny (np. tymczasowe wyłączenie usługi Rublon na VPN do czasu naprawienia integracji). Zawsze staraj się ustalić, czy problem ma zasięg globalny, czy jest odosobniony, ponieważ w zależności od tego reakcja będzie się różniła.

Scenariusz A: Awaria określonej metody uwierzytelniania

Przykład: Serwis dostarczania wiadomości SMS usługi Rublon ma awarię i kody wysyłane SMS-em nie docierają do użytkowników. Inne metody (powiadomienia push na telefon, kody TOTP z aplikacji mobilnej, linki wysyłane e-mailem, połączenia telefoniczne) działają poprawnie.

Skutek: Użytkownicy, którzy polegają wyłącznie na metodzie, której dotyczy problem (w tym przykładzie SMS), nie będą mogli ukończyć uwierzytelniania MFA. Mogą poprosić o kod SMS i nigdy go nie otrzymać. Nie będzie to miało wpływu na użytkowników korzystających z innych metod.

Wykrycie: Strona statusu Rublon pokaże problem z dostarczaniem SMS-ów (na liście komponentów usługa *„SMS Message Delivery”* będzie oznaczona jako zdegradowana). Użytkownicy będą zgłaszać: *„Nie otrzymuję kodu”*.

Opcje reakcji:

- **Zaproponuj alternatywną metodę uwierzytelniania:** Poinformuj użytkowników o zaistniałym problemie i poproś, by skorzystali z alternatywnej metody uwierzytelniania, takiej jak Powiadomienie mobilne czy Link e-mail. Wymaga to, aby użytkownicy mieli inny zarejestrowany uwierzytelniacz. W idealnym przypadku wszyscy użytkownicy powinni być zachęcani do posiadania co najmniej dwóch metod uwierzytelniania (np. aplikacja Rublon Authenticator plus numer telefonu, albo klucz bezpieczeństwa FIDO2 plus aplikacja generująca kody), aby mieć opcję zapasową.
- **Skorzystaj z kodu pominięcia Bypass Code:** Jeśli żadna alternatywna metoda nie wchodzi w grę, a dany użytkownik pilnie potrzebuje dostępu, administrator może wygenerować kod pominięcia Bypass Code (jednorazowy kod pomijający MFA) oraz poinstruować użytkownika jak korzystać z kodów pominięcia.
- **Sprawdź stronę statusu Rublon:** Obserwuj stronę statusu Rublon w oczekiwaniu na komunikat o rozwiązaniu problemu. Jeśli subskrybujesz powiadomienia ze strony statusowej, otrzymasz automatyczny e-mail, gdy tylko problem zostanie rozwiązany. Tego typu awarie pojedynczych metod są zazwyczaj szybko rozwiązywane przez zewnętrznego dostawcę usług.
- **Nie zmieniaj trybu Fail Mode:** W tym scenariuszu zazwyczaj nie ma potrzeby zmiany trybu Fail Mode, ponieważ uwierzytelnianie MFA nadal działa. Należy skupić się na zapewnieniu użytkownikom jasnych wskazówek.

Scenariusz B: Ogólne spowolnienie usługi lub częściowa awaria

Przykład: Interfejs Rublon API odpowiada powoli lub niektóre żądania uwierzytelnienia kończą się sporadycznymi błędami. Użytkownicy zgłaszają, że czasami ich monit MFA wygasa (timeout) lub pojawiają się błędy, ale po kilku próbach udaje się zalogować.

Skutek: Uwierzytelnianie jest zawodne i niestabilne. Może to być frustrujące dla użytkowników i spowalniać ich pracę. Problem nie blokuje całkowicie dostępu, ale powoduje opóźnienia i zamieszanie.

Wykrycie: Użytkownicy będą zgłaszać, że *„MFA nie działa za każdym razem”* lub *„MFA działa wolno”*. Strona statusu Rublon będzie pokazywać degradację jednej lub kilku usług.

Opcje reakcji:

- **Sprawdź stronę statusu Rublon:** Problemy związane z degradacją są rozwiązywane stosunkowo szybko (często w ciągu kilku minut do godziny). Z góry ustal, jak długo jesteś w stanie funkcjonować w stanie zdegradowanym, zanim podejmiesz bardziej zdecydowane kroki. (np. wprowadź plan pomijania po 30 minutach utrzymujących się poważnych problemów z logowaniem).
- **Uspokój użytkowników:** Jeśli problem jest niewielki, a strona stanu wskazuje na szybkie rozwiązanie, najlepszym podejściem może być powiadomienie użytkowników, że *„MFA ma obecnie sporadyczne problemy, prosimy o ponowienie próby, jeśli się nie powiedzie, i spodziewaj się możliwych opóźnień”*. Czasami samo określenie oczekiwań pomaga zmniejszyć liczbę zgłoszeń do działu pomocy technicznej.
- **Tymczasowo pomijaj MFA:** Jeśli zdegradowany stan usługi poważnie utrudnia prowadzenie działalności (logowanie trwa zbyt długo i praca zostaje zatrzymana), możesz zastosować obejście do czasu rozwiązania problemu:
    - Zmień status wszystkich lub wybranych użytkowników na **Bypass**.
    - Zbiorczo dodaj użytkowników do grupy o statusie **Bypass**.
    - Włącz tryb **Fail Safe** (FailMode=bypass) w jednym lub kilku konektorach Rublon i dodaj regułę zapory, która blokuje ruch do **core.rublon.net** na porcie TCP 443, aby wymusić pomijanie MFA.
    - Jeśli jest to absolutnie konieczne, tymczasowo wyłącz lub odinstaluj konektory Rublon (**niezalecane**).
    - Upewnij się, że wszelkie zmiany są przekazywane zespołowi, aby wszyscy wiedzieli, że usługa MFA została celowo pominięta, oraz **nie zapomnij wycofać zmian** po rozwiązaniu incydentu.

11. Szablony komunikatów do użytkowników końcowych

Jasna komunikacja z użytkownikami końcowymi jest niezwykle ważna podczas awarii lub zakłóceń działania usługi. Użytkownicy mogą wpadać w panikę lub zasypywać dział wsparcia zgłoszeniami, jeśli nagle nie mogą się zalogować albo ich monity MFA zachowują się inaczej niż zwykle. Posiadanie z wyprzedzeniem przygotowanych komunikatów pozwala szybko poinformować użytkowników o tym, co się dzieje i co (o ile cokolwiek) powinni zrobić. Poniżej przedstawiamy przyjazne, profesjonalnie sformułowane szablony wiadomości, które możesz dostosować i rozesłać. Możesz je przekazać e-mailem, poprzez czat lub innym kanałem komunikacji odpowiednim dla Twojej organizacji.

Decydowanie o tym, kiedy powiadomić użytkowników:

Zanim skorzystasz z poniższych szablonów, zastanów się, kiedy je wysłać. Możesz zdecydować powiadomić użytkowników od razu, gdy tylko problem zostanie potwierdzony (zwłaszcza jeśli dotyczy on dużej liczby osób i krytycznych systemów). Możesz też wstrzymać się kilka minut, by sprawdzić, czy problem szybko sam ustąpi (aby uniknąć niepotrzebnego alarmu), szczególnie jeśli zdarza się to poza godzinami pracy lub dotyka tylko niewielkiej grupy użytkowników. Kieruj się zdrowym rozsądkiem, uwzględniając porę i krytyczność systemów (np. problem o 9:00 w poniedziałek wymaga szybkiej komunikacji; problem o północy w sobotę w systemie używanym tylko w dni powszednie może nie wymagać natychmiastowego alertu). Dodatkowo, jeśli spodziewasz się, że problem zostanie bardzo szybko rozwiązany (załóżmy, że strona statusu Rublon wskazuje na jednominutową przerwę techniczną), możesz zdecydować się wstrzymać, chyba że incydent się przedłuża.

Szablon 1: Ogólna awaria – tryb Fail Safe (pominięcie MFA)

Scenariusz: Interfejs Rublon API jest nieosiągalny lub jedna bądź więcej usług Rublon uległo degradacji. Jako rozwiązanie tymczasowe, włączono pominięcie MFA (Fail Safe), dzięki czemu użytkownicy mogą się na razie logować wyłącznie przy użyciu uwierzytelniania podstawowego.

Temat: Problemy z uwierzytelnianiem - usługa MFA tymczasowo wyłączona

Treść:
Nasz dostawca uwierzytelniania wieloskładnikowego (Rublon) zgłasza problem ze swoimi usługami. Aby zapewnić wszystkim możliwość kontynuowania pracy, **tymczasowo znieśliśmy wymóg uwierzytelniania Rublon MFA przy logowaniu**. Oznacza to, że nie będziesz teraz proszony o podanie drugiego czynnika i zalogujesz się przy użyciu tylko nazwy użytkownika i hasła. Prosimy o zachowanie czujności w kwestii bezpieczeństwa w tym czasie. Po rozwiązaniu problemu **przywrócimy wymóg MFA**. Poinformujemy Cię, kiedy to nastąpi.

Szablon 2: Ogólna awaria – tryb Fail Secure (brak pominięcia)

Scenariusz: Interfejs Rublon API jest nieosiągalny lub jedna bądź więcej usług Rublon uległo degradacji. Uwierzytelnianie MFA **nie jest** pomijane (pozostawiono włączony tryb Fail Secure). Użytkownicy nie będą mieli dostępu do chronionych systemów, dopóki problem nie zostanie rozwiązany.

Temat: Problemy z uwierzytelnianiem - dostęp tymczasowo wstrzymany

Treść:
Nasz dostawca uwierzytelniania wieloskładnikowego (Rublon) zgłasza problem ze swoimi usługami. W rezultacie logowanie do **<dotknięte systemy>** nie jest obecnie możliwe. Jest to umyślnie wprowadzony środek ostrożności ze względu na wrażliwy charakter tych systemów - nie możemy udzielić do nich dostępu bez MFA. Rozumiemy, że jest to frustrujące, dlatego nasz zespół IT ściśle współpracuje z firmą Rublon, aby jak najszybciej rozwiązać ten problem. **Prosimy nie podejmować ponownych prób logowania, dopóki nie ogłosimy przywrócenia dostępu - obecnie i tak się one nie powiodą.** Przekażemy aktualizację, gdy tylko problem zostanie rozwiązany lub gdy pojawi się alternatywna metoda dostępu.

Szablon 3: Problem z określoną metodą uwierzytelniania

Scenariusz: Określona metoda MFA nie działa (ale inne metody działają). Na przykład, uwierzytelnianie e-mail nie działa, ale inne metody (SMS, połączenia telefoniczne) działają. Inny przykład: dostarczanie SMS-ów jest mocno opóźnione.

Temat: Komunikat serwisowy MFA - skorzystaj z alternatywnej metody uwierzytelnienia

Treść:
Nasz dostawca uwierzytelniania wieloskładnikowego (Rublon) zgłasza problem z metodą uwierzytelniania **<dotknięta metoda>**. Oznacza to, że możesz mieć problemy z dokończeniem logowania, jeśli w drugim etapie uwierzytelniania zwykle używasz **<push/SMS/telefon>**. Tymczasowym rozwiązaniem jest skorzystanie z metody **<metoda alternatywna>**. Monitorujemy sytuację i poinformujemy Cię, kiedy **<dotknięta metoda>** znów będzie działać normalnie. Jeśli nie masz pewności, jak skorzystać z alternatywnej metody lub nadal nie możesz się zalogować, skontaktuj się z działem obsługi IT w celu uzyskania pomocy.

Dodatkowe wskazówki komunikacyjne

- Wyślij wiadomość uzupełniającą, gdy problem zostanie rozwiązany. Na przykład: *„Problem z usługą MFA został rozwiązany. Rublon MFA znów działa prawidłowo. Jeśli korzystałeś z zapasowej metody uwierzytelniania, możesz powrócić do preferowanej metody. Dziękujemy za cierpliwość."*
- Zachowaj spokojny i pomocny ton wypowiedzi. Podczas awarii użytkownicy mogą być zaniepokojeni (*„Nie mogę zalogować się do pracy, co teraz?"*). Zapewnij ich, że zespół IT już nad tym pracuje, i przekaż, jakie kroki powinni (lub nie powinni) podejmować.
- Jeśli awaria dotyczy tylko podzbioru użytkowników (na przykład konkretnego oddziału lub grupy), dostosuj komunikat do tej właśnie grupy, aby nie wprowadzać zamieszania.
- Jeżeli awaria się przedłuża lub zmienił się sposób jej obejścia, przekazuj użytkownikom regularne aktualizacje (np. *„Usługa MFA nadal nie działa (stan na 11:30"). W dalszym ciągu pomijamy MFA. Następna aktualizacja za godzinę lub wcześniej, jeśli pojawią się nowe informacje."*).

12. Przegląd po incydencie

Po każdej awarii lub degradacji usługi Rublon warto przeprowadzić krótkie podsumowanie w gronie zespołu IT lub zespołu bezpieczeństwa. Pozwala to zidentyfikować, co zadziałało dobrze, a co można udoskonalić następnym razem.

Pytania do rozważenia:

- Czy użytkownicy mieli dostęp do systemów zgodnie z oczekiwaniami, biorąc pod uwagę ustawiony tryb Fail Mode?
- Czy administratorzy zastosowali odpowiednie kroki, takie jak przełączenie na tryb bypass lub użycie alternatywnych metod?
- Czy komunikacja do użytkowników była jasna i przekazana terminowo?
- Czy wszystkie wyjątki od zasad bezpieczeństwa (np. tymczasowe pominięcie MFA) zostały odpowiednio odnotowane i przywrócone do stanu normalnego?

Na podstawie wyników takiego przeglądu zaktualizuj swoją dokumentację procedur, szablony komunikatów oraz ustawienia konfiguracji. Regularne analizowanie realnych incydentów sprawia, że Twój plan ciągłości działania pozostaje aktualny, wykonalny i dostosowany do zmieniających się potrzeb Twojej organizacji.

13. Często zadawane pytania (FAQ)

Poniżej znajduje się kilka częstych pytań związanych z przestojami usługi Rublon MFA i ciągłością działania, wraz z odpowiedziami:

P1: Jak mogę sprawdzić, czy konektor wszedł w „tryb Fail Mode” (tj. pomija MFA lub odmawia dostępu z powodu nieosiągalności interfejsu Rublon API)?

Odp.: Istnieje kilka wskaźników:

Jeśli konektor jest ustawiony na tryb **Fail Safe** (FailMode=bypass), najbardziej oczywistym znakiem jest to, że użytkownicy logują się bez konieczności przejścia przez proces uwierzytelniania MFA w sytuacji, gdy normalnie byłoby to konieczne.

Przykładowo, jeśli nagle nikt nie jest proszony o podanie drugiego czynnika przy logowaniu, prawdopodobnie konektor zadziałał w trybie „awaryjnego otwarcia” (pomijania) – albo z powodu awarii usługi, albo z powodu problemu z konfiguracją. Z kolei jeśli aktywny jest tryb **Fail Secure** (FailMode=deny), użytkownicy będą zgłaszać, że nie mogą się zalogować w ogóle.

Aby potwierdzić uruchomienie trybu Fail Mode od strony serwera, sprawdź konfigurację danego konektora. Przejrzyj też plik logów konektora – wiele konektorów Rublon zapisuje zdarzenie, gdy uruchamia się tryb awaryjny.

Obecnie interfejs Rublon API **nie** wysyła bezpośredniego alertu, gdy lokalny konektor przechodzi w tryb Fail Mode, ponieważ może nawet o tym nie wiedzieć, jeśli konektor nie będzie mógł się połączyć z interfejsem Rublon API. Zalecamy użycie systemu monitorowania lub SIEM do obserwacji logów krytycznych konektorów. Można na przykład ustawić alert w przypadku nagłego wzrostu liczby uwierzytelnień typu bypass”. Proaktywne monitorowanie może dać Ci wczesne ostrzeżenie, że coś jest nie tak.

P2: Czy Rublon MFA będzie działać, jeśli nie będzie dostępu do Internetu lub użytkownik będzie całkowicie offline?

Odp.: Zasadniczo nie. Rublon MFA jest usługą chmurową, więc w trakcie logowania klient musi połączyć się z serwerami Rublon. Jeśli brak jest łączności internetowej, krok MFA nie może zostać ukończony i zastosowany zostanie skonfigurowany tryb Fail Mode (albo przepuszczenie,

albo odmowa dostępu, w zależności od ustawień). Jednym godnym uwagi wyjątkiem jest **tryb Offline Mode dostępny w konektorze Rublon dla Windows**.

14. Załącznik A: Słownik kluczowych terminów

- **Interfejs Rublon API:** centralna usługa internetowa obsługująca żądania uwierzytelniania wieloskładnikowego.
- **Widok Rublon Prompt:** interaktywny ekran wyświetlany po pomyślnym uwierzytelnieniu podstawowym w aplikacjach zintegrowanych z Rublon (posiadających interfejs graficzny). Umożliwia użytkownikom wybór dostępnej metody uwierzytelnienia oraz rejestrację nowych urządzeń do MFA.
- **Uwierzytelnianie podstawowe:** Początkowy proces weryfikacji tożsamości użytkownika, gdy po raz pierwszy próbuje on uzyskać dostęp do systemu lub aplikacji, zwykle obejmujący podanie takich danych uwierzytelniających, jak nazwa użytkownika i hasło.
- **Uwierzytelnianie dodatkowe:** Następujący po uwierzytelnianiu podstawowym proces, który wprowadza dodatkową warstwę weryfikacji, zazwyczaj wykorzystując metody uwierzytelniania wieloskładnikowego (np. kody TOTP, powiadomienia push lub dane biometryczne), aby jeszcze dokładniej potwierdzić tożsamość użytkownika.
- **Drugi składnik:** Metoda weryfikacji używana w ramach uwierzytelniania wieloskładnikowego, stanowiąca uzupełnienie podstawowych danych uwierzytelniających (nazwa użytkownika + hasło). Może to być coś, co użytkownik posiada (np. telefon komórkowy) lub coś, czym użytkownik jest (np. odcisk palca).
- **Tryb Fail Mode:** opcja określająca, jak aplikacja ma się zachować, jeśli nie może skontaktować się z interfejsem Rublon API. Tryb Fail Mode może być ustawiony na Fail Safe (pominięcie MFA) lub Fail Secure (odmowa dostępu).
- **Fail Safe (pominięcie):** umożliwia użytkownikowi, który przeszedł uwierzytelnienie podstawowe, zalogowanie się bez MFA, jeżeli interfejs Rublon API jest nieosiągalny.

- **Fail Secure (odrzucenie):** odrzuca logowanie w całości, jeżeli nie można dokończyć uwierzytelnienia MFA.
- **Kod pominięcia Bypass Code:** jednorazowy kod, który administratorzy mogą wygenerować, aby pozwolić użytkownikowi zalogować się bez dokańczania uwierzytelniania MFA (np. gdy użytkownik utracił dostęp do urządzenia stanowiącego drugi czynnik uwierzytelniania).
- **Degradacja usługi:** częściowa awaria, podczas której interfejs Rublon API jest nadal osiągalny, ale jedna lub więcej usług MFA (np. konsola Rublon Admin Console, wysyłanie SMS-ów itp.) jest niedostępnych, działa wolno lub niestabilnie.

Rublon sp. z o.o.
ul. Stanisława Wyspiańskiego 11
65-036 Zielona Góra

www.rublon.pl